Navy Strategy for Achieving Information Dominance

2013-2017

Optimizing Navy's Primacy in the Maritime and Information Domains

Report Documentation Page

1. REPORT DATE **2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2017**

4. TITLE AND SUBTITLE **Navy Strategy for Achieving Information Dominance, 2013-2017**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Chief of Naval Operations, Information Dominance,Room: 4E360,2000 Navy Pentagon,Washington,DC, 20350**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**17**	

Foreword

The global spread of sophisticated information technology is changing the speed at which warfare is conducted. Through the early adoption of high-tech data links, worldwide communication networks, people skills and advanced reconnaissance and surveillance systems, the U.S. Navy has long enjoyed information superiority over potential adversaries. However, our advantage is eroding as more nations, transnational criminal organizations and non-state actors are acquiring and employing more advanced computing and networked systems. Many, in fact, are actively exploiting our networks and developing the means to challenge our technological edge.

To meet these challenges, the Navy is aggressively pursuing a multi-faceted approach to warfighting which ensures our information superiority in future conflict. This Navy Strategy for Achieving Information Dominance frames the approach and will guide the development of our information capabilities and their integration into the fleet. It reinforces our consolidation of information-related programs, resources and manpower under a single sponsor, and accelerates the work accomplished over the last three years to integrate Information Dominance into our Navy as a core warfighting competency. Finally, it bolsters our efforts to master the cyberspace domain and the electromagnetic spectrum, just as we have mastered the physical domains of the maritime battlespace

Joining surface, subsurface, air and special warfare, information dominance is our newest warfighting pillar, delivering the non-kinetic complement to our kinetic capabilities in the cyberspace domain. The Information Dominance pillar can be our most powerful asset, or it can be our greatest liability. If we integrate it intelligently, and if we execute it correctly, we will be able to seize the operational initiative, gain tactical advantage, and win future battles with overwhelming speed.

Information Dominance is indispensable to our Navy, enabling the Navy to fight and win today, while ensuring the ability to win tomorrow. It is imperative that we embrace Navy Information Dominance deliberately and expeditiously, and always be ready to fight. Please join us in executing this strategy.

KENDALL L. CARD
Vice Admiral, U.S. Navy
Deputy Chief of Naval Operations
For Information Dominance

MICHAEL S. ROGERS
Vice Admiral, U.S. Navy
Commander, Fleet Cyber Command/
Commander, TENTH Fleet

Executive Summary

The continuing evolution in information technology presents both opportunities and challenges for the U.S. Navy. Information is becoming increasingly central to all aspects of maritime warfighting and is core to the Navy's strategic, operational and tactical missions of sea control, power projection, deterrence and forward presence. Whether characterized as intelligence, surveillance, reconnaissance, networks, communications, space, cyber, meteorology, oceanography, or electronic warfare, the Navy is inextricably and irreversibly dependent on information. Information provides a source of power but can also be an incapacitating weakness if not protected. Mastering the information domain is critical to the Navy's future success.

Complicating the Navy's challenges are the ways in which information has evolved in the modern era. Although historically employed as an enabler of combat (information "in" warfare), information is being deployed more and more as a weapon (information "as" warfare). Cyberspace is the information warfighting domain, and the network and the electromagnetic spectrum comprise the battlespace. This continued transformation of information as both a weapon and an enabler in combat is driving an altogether unique warfighting capability that the U.S. Navy is calling Information Dominance.

Defined as *the operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize warfighting effects,* Navy Information Dominance has become a leading Service priority. In 2009 the Navy consolidated information-related programs, resources, and manpower in order to organize, unify and concentrate its information capabilities. This *Strategy for Achieving Information Dominance* provides the framework through which the Navy's information capabilities will be mainstreamed into the Navy's culture as a distinct warfighting discipline.

The strategy focuses on the three fundamental Information Dominance capabilities of **Assured Command and Control, Battlespace Awareness, and Integrated Fires**, and sets forth the following major goals for the 2013–2017 timeframe:

- Strong and Secure Navy Command and Control;
- Persistent, Predictive Battlespace Awareness;
- Integrated Combat Information;
- Integrated Kinetic and Non-kinetic Fires;
- Information Dominance as a Warfighting Discipline.

Future enabling capabilities will be outlined in the follow-on Navy Information Dominance Roadmap, 2013–2028. Through this document, the Navy sets its sights on attaining decision superiority for the Navy-Marine Corps Team, and joint and coalition commanders at multiple levels. It lays the practical foundations for mastering the cyberspace domain. This strategy will be reviewed and revalidated annually to ensure its continued relevance to current and future Navy operations.

Finally, this strategy is consistent with the 2012 defense strategic guidance, *Sustaining U.S. Leadership: Priorities for 21st Century Defense,* the 2012 Chairman's *Strategic Direction for the Joint Force*, and the Chief of Naval Operations' *Sailing Directions* and *Navigation Plan.*
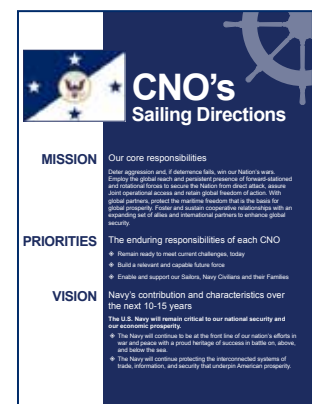
The Ascendancy & Centrality of Information

Any new strategy should begin with the question, *"What has changed?"* As an element of modern warfare, information has emerged as a center of gravity for military commanders and features prominently in the nation's strategy. Whether manifested as combat enabler, warfare domain, weapon, threat or warfighting discipline, information has become an indispensable component which must be planned, programmed, resourced, practiced, and mastered for military success. To comprehend the importance of information in this context, it is essential to understand its evolving aspects.

Information as enabler. For millennia, access to superior information has been an essential determinant for success in battle. The importance of acquiring, exploiting, protecting and moving combat information remains unchanged in the 21st Century. *What has changed* is the instantaneous speed and massive volume at which information can be discovered, accessed, processed, exploited and disseminated, regardless of its origin or intended destination. Enabled by advanced technology, the military force that senses, processes and delivers information more efficiently than its adversary will enjoy enhanced and predictive battlespace awareness, better command and control (C2), and greater decisional agility.

Information as warfare domain. Warfare has historically been fought in the physical domains involving the land, sea, air and space. With the advent of advanced radio, computer and network technology, *what has changed* is the growing importance of the electromagnetic (EM) spectrum and cyberspace as not only enablers of the physical domains, but as a warfighting domain in its own right. The cyberspace domain is likely to figure largely in future conflicts and crisis. The military force that dominates this domain and effectively "fights" on its network and in the EM spectrum—just as it "fights" on ships and aircraft—will also develop and maintain an advantage over its adversaries.

Information as weapon. Because the Navy is inextricably dependent on its networks, and because of its centrality to warfighting, the network and its components (information, intelligence, technology, people, etc.) are, in effect, a combat system, a platform and a target. As the 1990's concept of Network Centric Warfare expanded and as technology advanced, *what has changed* is that we now have a ubiquitous network and EM spectrum from which to launch information as a weapon. The military force that uses its networks and cyberspace to exploit and attack the vulnerabilities of its adversaries will maintain a combat advantage. Moreover, the military force that integrates non-kinetic or electromagnetic strike options with traditional kinetic fires will compound its warfighting effects.

Information as threat. The reliance on advanced information systems in warfare, however, presents challenges. Over the past several years, the Navy has become ever more dependent on its information technology (IT) as we pace evolving computing advances, communication technologies, and new information systems. Knowing this, adversaries have begun to develop, acquire and field modern, state-of-the-art information technologies of their own to:

- Exploit seams within the Department of Defense's (DoD) worldwide military networks;
- Disrupt the U.S. Navy's dependence on IT and its over-the-horizon intelligence, C2 and combat systems;
- Improve their situational awareness of U.S. Navy ship and aircraft movements;
- Coordinate their dispersed forces for long-range military engagements at sea.

The Navy's networks today remain vulnerable and are under near-continuous attack. Foreign cyberspace threats, combined with the worldwide proliferation of advanced long-range weapon systems and other asymmetric capabilities, have the potential to reduce the Navy's technological and operational advantages.

Information as warfighting discipline. Until 2009, the information-intensive communities of Oceanography, Information Warfare, Information Professional, Intelligence and the Space Cadre were treated principally as individual enablers necessary to support the Navy's traditional warfighting pillars. Recognizing the enhanced combat power of fusing the Navy's disparate information capabilities and manpower, the Chief of Naval Operations consolidated these communities under the banner of Information Dominance. Navy's aggregate information capability has begun to emerge as a modern warfighting enterprise, and serves as a potent asymmetric complement to its kinetic warfare capabilities. Among its myriad purposes, this strategy serves to further define and establish Information Dominance as the Navy's newest warfighting discipline in support of the Navy's primary tenet of Warfighting First.

"Control of information—much of it through the electromagnetic spectrum—is already growing more important than the control of territory in modern warfare."

Admiral Jonathan Greenert
Chief of Naval Operations
23 September 2011

INFORMATION DOMINANCE CHALLENGE

In view of the exponential growth and global pervasiveness of IT, its comparatively low cost relative to conventional warfare systems, and the ease with which it can be "weaponized" for asymmetric purposes, the Navy faces enormous challenges in the future maritime operating environment. Furthermore, given information's prominence in national, joint, coalition and Navy strategic objectives, it is imperative that the Navy's information "portfolio" be organized in a way that achieves and protects its real warfighting capability. In other words, the constituent components (e.g., resources, capabilities, governance, tactics, techniques, procedures) must be marshaled, aligned with Doctrine, Organization, Training, Materiel, Logistics, Personnel and Facilities, and employed for optimum effect. Just as we are masters of the maritime domain, to win in future conflict *we must also master the information domain.*

KEY TERMS AND CONCEPTS

Enabling and implementing the Navy's information portfolio to achieve dominance requires clearly stated terms and concepts. The following key terms and concepts are critical for a foundational understanding:

Mission. The Navy's Information Dominance professionals will:
- Maintain superior knowledge of the battlespace;
- Provide our operating forces with sufficient over-match in wartime command and control;
- Ensure our ability to deeply infiltrate and understand the inner workings of our adversaries, and

- Project power through and across the network in support of forward-deployed Navy, joint and coalition forces.

Vision. The Navy's Information Dominance vision is to provide assured maritime command and control and superior battlespace awareness to enable sustained, integrated fires across the full spectrum of 21st Century maritime warfare.

Definition: Information Dominance is defined as the operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize warfighting effects.

Three Fundamental Capabilities. At its core, Information Dominance hinges on the three fundamental capabilities of Assured C2, Battlespace Awareness, and Integrated Fires. When achieved in the aggregate, these capabilities allow Navy commanders to operate freely within the information domain, and to stay well ahead of the adversary's decision cycle.

Assured C2. The Navy must assure its ability to command and control forces. This requires capabilities that enable commanders to:
- Exchange orders and responses with subordinates;
- Understand the disposition of friendly forces;
- Target and conduct strikes as part of the joint force; and then
- Assess the result of those strikes.

Sensing the environment, understanding our adversaries and operating and defending our communications and networked systems are inextricably linked to the assurance of C2.

Battlespace Awareness. This is the traditional mission of the Information Dominance Corps and the constituent components of meteorology, oceanography, intelligence, cryptology, communications, networks, space and electronic warfare (EW). It includes:

- Persistent surveillance of the maritime and information battlespace;
- Penetrating knowledge of the capabilities and intent of our adversaries;
- An understanding of when, where, and how our adversaries operate; and
- Expertise within the electromagnetic spectrum.

When synchronized, these skills and knowledge attributes provide the target acquisition and targeting solutions necessary to apply force, both kinetic and non-kinetic.

Integrated Fires. The Navy will use its networks, cyberspace and space capabilities to exploit and attack the vulnerabilities of its adversaries to achieve non-kinetic effects (i.e., fires). Just as importantly, we will expand options for forward-deployed Navy commanders by ensuring that non-kinetic alternatives are considered alongside with kinetic solutions.

A STRATEGY TO ACHIEVE INFORMATION DOMINANCE

In response to the challenge of mastering the information domain and consistent with the mission and vision stated above, this document establishes a framework for the integration of the Navy's information-based programs, capabilities, expertise, resources and operations. The strategy's goals and objectives will be developed further in the Navy's Information Dominance Roadmap, 2013–2028.

GOAL 1: ROBUST COMMUNICATIONS FOR NAVY COMMAND AND CONTROL

To succeed in contested environments, particularly in Anti-Access/Area Denial (A2/AD) scenarios, the Navy must improve the adaptability and security of its information infrastructure by strengthening governance, setting and enforcing Navy-wide standards, and building C2 paths that are adaptable and resistant to cyber and electronic attack.

Objective 1.1
Assure communications paths through dynamic networking
The Navy's networks must be sufficiently agile to maintain freedom of action for Navy users in cyberspace. They must connect the right user (ships, aircraft, submarines, sensors, warfighters, etc.) with the information and decision making tools necessary to dominate the battlespace and sustain those connections.

Objective 1.2
Manage and assure electromagnetic spectrum operation
To maintain an operational advantage, the Navy will ensure the continued use of space assets and essential portions of the electromagnetic spectrum in all threat environments.

Objective 1.3
Build a resilient and assured C2 infrastructure that supports naval forces worldwide
An adaptable enterprise architecture, strong governance and operational control of our networks will provide sufficient C2 paths and capacity without regard to where the Navy is operating.

GOAL 2: PERSISTENT, PREDICTIVE BATTLESPACE AWARENESS

To win, our warfighters must have superior, predictive knowledge of both their physical and virtual battlespace. They must know the adversary's specific situation, capabilities, and perspective in order to successfully acquire and deter or engage targets in a timely manner. Therefore, persistent, end-to-end, theater-focused Intelligence, Surveillance and Reconnaissance (ISR) is crucial. We will continue to effectively coordinate with national, joint and coalition partners to fully leverage all available ISR capability.

Objective 2.1
Understand, forecast and exploit the physical maritime environment
The Navy will understand and characterize for the commander how the physical environment may impact the mission. This understanding will be also be seamlessly incorporated into Navy operational and mission planning.

Objective 2.2
Manage sensor employment against prioritized intelligence requirements
The duration, dwell, range, and access of unmanned vehicles demands greater management of sensors to ensure collection is tailored to operational need. The exponential increase in data generated by these assets will require that sufficient processing capability (both manpower and systems) exists to convert the collected information into intelligence. Similarly, advances in space sensor systems will likewise generate greater amounts of data that must be actively managed, processed and synthesized into the larger common operational picture.

Objective 2.3
Know the adversary
The Navy will create decisional advantage by exploiting all sources and its unique forward presence to assess adversary disposition, operations, networks, intent, tactics, techniques, procedures and vulnerabilities. To win in the maritime domain, we will master the means of locating, tracking and penetrating our adversaries, and then translate that associated knowledge into timely, actionable intelligence for our forward-deployed forces.

Objective 2.4
Integrate and leverage National, Joint and Coalition intelligence
We will use a federated approach to fully access the intelligence community, amplifying our traditional combat capabilities and expanding warfighting options for both Navy and Joint commanders.

GOAL 3: INTEGRATED COMBAT INFORMATION

From planning to execution to battle damage assessment, we will provide Navy commanders with a high degree of informational fidelity in complex, data-intensive environments. This will allow for greater speed of command and also enable more precise targeting solutions.

Objective 3.1
Assure C2 in all levels of conflict
As noted in Goal 1, assured C2 is critical to the delivery of fires in the information age. To effectively employ and control their forces, Navy commanders must be able to exchange orders with forward operating subordinates, perform targeting, conduct strikes, and synchronize force actions, all in highly fluid and dynamic circumstances.

Objective 3.2
Incorporate Information Dominance-related capabilities into operational plans
Consistent with the aforementioned concepts of "information in warfare" and "information as warfare," information-intensive capabilities will be deliberately "mainstreamed" into Navy's operational and mission planning to support our emphasis on Warfighting First.

Objective 3.3
Integrate all-source information across kill chains
Outputs from all sensors in all domains will be accessible in time to facilitate freedom of action, targeting, and the employment of weapons, both kinetic and non-kinetic. Disparate information sources will necessarily span physical locations, security classifications and Navy warfighting domains, but they must be synthesized to create actionable knowledge. This knowledge must be made available to decision makers at the time and in the format of their choosing.

GOAL 4: INTEGRATED KINETIC AND NON-KINETIC FIRES

To multiply warfighting effects, the Navy will integrate kinetic and non-kinetic fires. To this end, the Navy will expand and strengthen its operations within cyberspace and the electromagnetic spectrum. To dominate in these areas, the Navy will further develop its cyber workforce, bolster related research and development, and refine its governance, policy and TTP. Specifically, we must improve our active network defense and improve our offensive cyber capability. Likewise, the Navy must continue to advance its EW capabilities in order to disrupt adversary surveillance, targeting, and C2, and effectively counter anti-ship cruise missiles and ballistic missiles alike.

Objective 4.1
Advance electromagnetic capabilities
The Navy will modernize and integrate its lethal and non-lethal EW capabilities into all phases and levels of kinetic maritime operations while deconflicting and optimizing its operations in the electromagnetic spectrum, from radars to large-scale communications to individual data links. Such capabilities will advance the emerging Navy concept of conducting Electromagnetic Maneuver Warfare.

Objective 4.2
Integrate Cyberspace Operations with Fleet Operations
To deliver comprehensive fires, the Navy must strengthen and synthesize cyberspace operations with kinetic fleet operations. Blending these operational arts will yield an enhanced combat system that can exploit, influence, deny, degrade, disrupt and—if need be—physically destroy an adversary's power.

GOAL 5: INFORMATION DOMINANCE AS WARFIGHTING DISCIPLINE

As the Navy adjusts and adapts to the evolution of technology, we are building rigorous doctrine and providing tactics, techniques and procedures. We will continue to build the highly specialized knowledge and advanced technical skills required to operate, maintain and manage modern technology and "fight" the network. The Navy has a dedicated community of professionals trained and educated in the "arts" of information superiority. This Information Dominance Corps is likewise creating its own warfighting culture consistent with the Navy's historic traditions, but focused on mastering non-kinetic warfare in the non-physical, man-made cyberspace domain.

Objective 5.1
Incorporate Information Dominance into Navy warfighting doctrine and tactics
Navy doctrine and tactics will be updated to reflect Information Dominance concepts, capabilities and warfighting principles.

Objective 5.2
Integrate Information Dominance tenets into Fleet operations
Fleet training, exercises and operations will stress information-related capabilities and scenarios to ensure realistic preparation and amass practical experience underway.

Objective 5.3
Develop, manage, train and fully integrate the Information Dominance Corps (IDC)
The IDC now constitutes a total force professional community (officer, enlisted and civilian) that specializes in all facets of Information Dominance. This corps will be trained, managed and ready to provide the skills Navy requires to fight in the cyberspace domain.

THE INFORMATION DOMINANCE CORPS

People are the foundation of the Navy, and they must be trained and empowered to be ready to execute assigned missions. The Navy created the IDC as a means of leveraging the specialized skills of its information workforce and synthesizing the value of each IDC sub-community into a more effective warfighting capability.

Each member will receive an IDC introduction that frames the broad capabilities of ID, demonstrates the relevance of the capabilities to Navy operations, and reinforces how the member's individual contributions fit in the larger context. Whether military or civilian, each member will not only understand his or her role within their respective IDC sub-community or discipline (i.e., Oceanography, Meteorology, Information Warfare, Communications, Networks, Intelligence, etc.), but how their sub-community and their individual work relates to the other ID disciplines, and adds value to Navy missions.

This initial familiarization will be followed by specialization within the IDC's sub-communities and include training in TTPs, as well as the operational experience that provides unique value to Navy commanders. It is during this extended career phase that the Navy develops the experts and expertise that the IDC has historically provided, indeed what the IDC's component communities are traditionally known for. At more senior levels, members will emerge from their parent discipline and assume leadership positions within other IDC sub-communities. The aggregate impact of this cross-detailing is a combat-ready corps with a greater understanding of Information Dominance as a warfighting discipline, and a trained workforce more capable of integrating information effects into the decision-maker's planning and operations.

Navy leaders both inside and outside the IDC can expect the same specialized, unique expertise from the IDC. Under this reformed construct however, they can also expect senior professionals with the broadened knowledge, expertise and experience necessary to draw on all aspects of the information realm in support of the commander. In this way, the Navy will maintain freedom of action in the information domain, enhance the impact of kinetic operations, and deliver direct information effects against our adversaries.

THE WAY AHEAD

The Navy's success in future crises and conflicts depends increasingly on the speed, security, and adaptability of our C2, the depth and breadth of our battlespace awareness, and the effectiveness of our integrated fires. In implementing this strategy's goals and objectives, the IDC will remain ready to fight and win within the cyberspace domain. We will not only set our sights on maintaining decision superiority for our forward-deployed Navy-Marine Corps Team, and Joint and coalition commanders, we will lay the practical foundations for mastering information throughout cyberspace.

In support of this *Navy Strategy for Achieving Information Dominance*, a number of related Navy documents will be forthcoming in the near future to include: the *Navy Information Dominance Roadmap, 2013-2028*; the *Navy IDC Human Capital Strategy, 2013-2027*; *Navy Cyber Power 2020*; the *Naval Intelligence Strategy, 2013-2020*; and, the 2013 *Navy Space Strategy*. Within this integrated framework, the Navy begins in earnest the process of marshaling its resources, galvanizing the workforce, and aligning Navy's Information Dominance capabilities to fully enable the Navy's primary tenet of Warfighting First.